



Homeland Security

Daily Open Source Infrastructure Report

26 June 2015

Top Stories

- Fiat Chrysler is recalling 164,000 model year 2014 – 2015 Jeep Cherokee vehicles worldwide to address an issue in which water could get into the vehicle's power rear lift gate controls, posing a risk of fire. – *Associated Press* (See item [5](#))
- Authorities arrested a second Clinton Correctional Facility prison guard June 24 for allegedly trading tools to the escaped convicts in exchange for artwork. – *NBC News* (See item [17](#))
- European authorities from six countries, Europol, and Eurojust arrested five suspects in Ukraine believe to be part of a major cybercriminal ring that infected tens of thousands of users' computers worldwide with banking Trojans. – *Help Net Security* (See item [22](#))
- Ionia County, Michigan declared a state of emergency after a June 22 tornado heavily damaged 70 homes, more than 12 businesses, and at least 4 churches. – *Lansing State Journal* (See item [35](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
- [Emergency Services](#)

Energy Sector

1. ***June 24, Newsroom America*** – (New Mexico) **U.S. requires Arizona and New Mexico plant owners to reduce emissions at Four Corners Power Plant.** The U.S. Department of Justice and the Environmental Protection Agency announced June 24 a \$168.2 million Federal Clean Air Act settlement with the companies that run the Four Corners coal fired power plant in New Mexico, requiring sulfur dioxide and nitrogen oxide pollution control upgrades, health and environmental mitigation projects, and payment of a civil penalty.

Source: <http://www.newsroomamerica.com/story/502489.html>

For additional stories, see items [24](#) and [31](#)

[\[Return to top\]](#)

Chemical Industry Sector

See item [31](#)

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

2. ***June 24, KFOR 4 Oklahoma City*** – (Oklahoma) **Gauge containing radioactive material stolen from Oklahoma City area.** The Oklahoma Department of Environmental Quality reported that a gauge containing radioactive material used to measure soil density and moisture content was stolen in Oklahoma City. The gauge poses no risk to human health unless it is unlocked or tampered with.
Source: <http://kfor.com/2015/06/24/gauge-containing-radioactive-material-stolen-from-oklahoma-city-area/>

For additional stories, see items [24](#) and [31](#)

[\[Return to top\]](#)

Critical Manufacturing Sector

3. ***June 24, U.S. Consumer Product Safety Commission*** – (National) **Positec Tool recalls Worx brand blower/vacs due to shock hazard.** Charlotte, North Carolina-based Positec Tool Corp., issued a recall June 24 for about 24,300 Worx brand electric blower/vacs due to an issue in which the grounded and ungrounded wiring in the tool could be reversed, posing a shock hazard. The product was distributed in Menards and Walmart stores nationwide from January – May.
Source: http://www.cpsc.gov/en/Recalls/2015/Positec-Tool-Recalls-Worx-Brand-Blower-Vacs/?utm_source=feedly&utm_medium=rss&utm_campaign=Recalls+RSS
4. ***June 24, U.S. Consumer Product Safety Commission*** – (National) **Bicycles with SR**

Suntour Bicycle forks recalled by SR Suntour due to crash hazard. SR Suntour issued a recall June 24 for about 68,000 Cannondale, Diamondback, Giant, GT, INA International, Schwinn, Scott and Trek brand bicycles with the company's bicycle forks due to an issue with a bolt that could cause the upper and lower forks to separate, causing the front wheel to come off. The products were sold at bicycle and sports stores and mass merchandisers nationwide from November 2014 – May 2015.

Source: http://www.cpsc.gov/en/Recalls/2015/Bicycles-with-SR-Suntour-Bicycle-Forks-Recalled-by-SR-Suntour/?utm_source=feedly&utm_medium=rss&utm_campaign=Recalls+RSS

5. ***June 24, Associated Press* – (National) Fiat Chrysler issues recall for 164,000 Jeep Cherokees.** Fiat Chrysler is recalling 164,000 model year 2014 – 2015 Jeep Cherokee vehicles worldwide to address a seal issue in which water could get into the vehicle's power rear lift gate controls, posing a risk of fire. The company will install shields and replace control modules exposed to water.

Source: http://www.nytimes.com/2015/06/25/business/fiat-chrysler-issues-recall-for-164000-jeep-cherokees.html?_r=0

For another story, see item [31](#)

[\[Return to top\]](#)

Defense Industrial Base Sector

6. ***June 25, United Press International* – (Arizona) F-16 fighter jet crashes in Arizona near Mexico border.** The U.S. Air National Guard reported that an F-16 Fighting Falcon jet from the 162nd Fighter Wing crashed June 24 during a night training mission, causing a large fire in Douglas, Arizona. The status of the pilot is unknown as U.S. Army personnel were sent to secure the crash site until Air Force officials arrive.

Source: http://www.upi.com/Top_News/US/2015/06/25/F-16-Fighter-jet-crashes-in-Arizona-near-Mexico-border/8661435225821/

[\[Return to top\]](#)

Financial Services Sector

7. ***June 23, New Hampshire Union Leader* – (New Hampshire) St. Mary's Bank issues new debit cards following breach.** St. Mary's Bank officials in Manchester, New Hampshire reported June 23 that the bank was reissuing 5,029 debit cards and replacing about \$25,000 in funds after about 160 cards were found to have been compromised in a breach.

Source: <http://www.unionleader.com/article/20150623/NEWS02/150629609>

For additional stories, see items [22](#) and [23](#)

[\[Return to top\]](#)

Transportation Systems Sector

8. ***June 25, Idaho State Journal*** – (Idaho) **Fiery crash – fuel tanker kills pedestrian in I-15 accident.** Northbound lanes of Interstate 15 in Blackfoot were shut down for more than 8 hours June 24 while crews cleared the scene after a semi-truck hauling fuel struck and killed a pedestrian crossing the northbound lanes.
Source: http://www.idahostatejournal.com/members/fiery-crash-fuel-tanker-kills-pedestrian-in-i--accident/article_f6d54cfa-1afe-11e5-ac06-fb045b30dac1.html
9. ***June 25, WLKY 32 Louisville*** – (Indiana) **6-vehicle crash closes I-65 for hours Wednesday.** The northbound lanes of Interstate 65 near mile marker 41.4 in Jackson County, Indiana were closed for over 5 hours June 24 while crews reconstructed and cleared the scene of a 6-vehicle accident.
Source: <http://www.wlky.com/news/accident-closes-northbound-lanes-of-i65-in-jackson-county/33755954>
10. ***June 24, Montgomery Advertiser*** – (International) **Flights delayed, canceled during Atlanta storms.** Atlanta-bound flights from across the South and flights from various cities in Mexico were rerouted to Montgomery Regional Airport while at least 11 outbound flights were canceled June 24 due to severe weather in the area. In addition, the airport reported June 24 that Metropolitan Atlanta Rapid Transit Authority was down following a power outage.
Source: <http://www.montgomeryadvertiser.com/story/news/2015/06/24/flights-delayed-cancelled-atlanta-storms/29240899/>
11. ***June 24, KOTV 6 Tulsa*** – (Oklahoma) **Fumes, air testing force two evacuations of Tulsa Airport Tower.** The control tower at Tulsa International Airport was evacuated twice June 24 after chemical fumes sickened 3 people and required crews to test the air. Sick employees were checked by on-site medics and due to the evacuations, some American Airlines flights were delayed.
Source: <http://www.news6.com/story/29401228/tulsa-international-airport-tower-evacuated>
12. ***June 24, Albany Democrat-Herald*** – (New York) **Two killed in wreck on Highway 34 west of Tangent.** Highway 34 near Looney Lane, south of Albany, was shut down for several hours June 24 due to a head-on collision that killed 2 and injured 1.
Source: http://democratherald.com/news/local/fatal-wreck-closes-highway-west-of-tangent/article_4fe47be2-4260-5805-b36a-3dd6fcd4e7d1.html

[\[Return to top\]](#)

Food and Agriculture Sector

Nothing to report

[\[Return to top\]](#)

Water and Wastewater Systems Sector

13. ***June 25, Glens Falls Post-Star*** – (New York) **1.2 million gallons of partially treated wastewater discharged into Hudson River.** The Washington County sewage treatment plant discharged 1.2 million gallons of partially treated wastewater into the Hudson River June 24 due to a mechanical issue at the plant. Officials are investigating its cause and the director of Washington County Sewer District II reported that there is no danger due to the spill.
Source: http://poststar.com/news/local/million-gallons-of-partially-treated-wastewater-discharged-into-hudson-river/article_f92e5e75-e6fc-5ff9-bb66-7e55063ee1c1.html

For additional stories, see items [24](#) and [31](#)

[\[Return to top\]](#)

Healthcare and Public Health Sector

14. ***June 25, Insurance Journal*** – (Georgia) **Georgia chiropractor indicted on 12 counts of insurance fraud.** The Georgia Insurance Commissioner announced June 25 that a Bibb County chiropractor has been charged with 12 counts of insurance fraud for allegedly submitting fraudulent bills to insurance companies for patient treatment which never occurred.
Source: <http://www.insurancejournal.com/news/southeast/2015/06/25/372934.htm>

[\[Return to top\]](#)

Government Facilities Sector

15. ***June 25, Securityweek*** – (International) **Leaked government credentials abundant on public Web.** Recorded Future released a report June 24 revealing that login credentials belonging to 47 U.S. Government agencies have been discovered on the public Web since November 2014, with the most affected agencies being the U.S. Department of Energy and Department of Commerce. The company shared its finding with affected agencies and is unsure if attackers attempted to leverage any stolen information.
Source: <http://www.securityweek.com/leaked-government-credentials-abundant-public-web>
16. ***June 24, Associated Press*** – (International) **New Mexican immigration fiasco as truck carrying hundreds of US visas is hijacked near the border.** The U.S. Embassy in Mexico announced June 24 the theft of a truck carrying hundreds of new U.S. visas which occurred in northern Mexico June 7. The intended holders have been notified of the robbery and given replacement cards, and an electronic alert has been issued to prevent illegal border crossings by the thieves.
Source:
http://hosted.ap.org/dynamic/stories/L/LT_MEXICO_US_VISA_THEFTS?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2015-06-24-11-22-38

[\[Return to top\]](#)

Emergency Services Sector

17. ***June 25, NBC News*** – (New York) **New York prison guard allegedly swapped artworks for tools.** Authorities arrested a second Clinton Correctional Facility prison guard June 24 for his role in the escape of two fugitive convicts. The guard allegedly accepted paintings from the convicts in exchange for tools, in which the paintings were allegedly burned and destroyed around the time of the escape.
Source: <http://www.nbcnews.com/storyline/new-york-prison-escape/new-york-prison-guard-gene-palmer-allegedly-took-escapees-paintings-n381531>
18. ***June 25, Associated Press*** – (Georgia) **3 indicted in college student's death in Georgia jail.** Two former Chatham County Jail workers and a health care contractor were charged June 24 in connection with the January death of a prison inmate in Savannah, Georgia.
Source: <http://abcnews.go.com/US/wireStory/indicted-college-students-death-georgia-jail-32006477>
19. ***June 25, Los Angeles Times*** – (California) **L.A. County deputies convicted in beating.** Three Los Angeles County sheriff's deputies were convicted June 24 of beating a handcuffed suspect and then lying to cover up the abuse in February 2011.
Source: <http://www.officer.com/news/14016380/three-la-county-deputies-convicted-in-beating>
20. ***June 24, Associated Press*** – (New York) **State prison in Auburn locked down, no reason given.** New York State Auburn Correctional Facility officials reported June 24 that a complete search of the prison and its inmates is underway, and that prisoners have been locked in their cells since June 19. They have not stated a specific reason for the lockdown or when it is expected to end.
Source:
http://www.syracuse.com/state/index.ssf/2015/06/state_prison_in_auburn_locked_down_no_reason_given.html

For another story, see item [32](#)

[\[Return to top\]](#)

Information Technology Sector

21. ***June 25, Help Net Security*** – (International) **Samsung disables Windows Update, undermines the security of your devices.** A security researcher discovered that the Samsung SW Update software for Microsoft Windows personal computers (PCs) runs an executable file upon start-up that disables Windows Update to prevent driver and update software conflicts, posing a security risk to users. Microsoft has reportedly contacted Samsung to address the issue.
Source: <http://www.net-security.org/secworld.php?id=18553>

22. ***June 25, Help Net Security*** – (International) **The downfall of a major cybercrime ring exploiting banking trojans.** European authorities from six countries along with Europol and Eurojust arrested five suspects in Ukraine believed to be part of a major cybercriminal ring that developed, exploited, and distributed Zeus and SpyEye malware, actively traded stolen credentials, laundered profits, and infected tens of thousands of users' computers worldwide with banking Trojans.
Source: http://www.net-security.org/malware_news.php?id=3064

23. ***June 25, Help Net Security*** – (International) **Why a Dyre infection leads to more than just stolen banking credentials.** Symantec reported that in addition to targeting banks, financial institutions, customers of electronic payment services, and users of digital currencies, cybercriminals are employing the Dyre Trojan to collect credentials for career and human resource Web sites, as well as Web hosting companies. The group using Dyre has reportedly targeted customers of over 1,000 organizations worldwide.
Source: http://www.net-security.org/malware_news.php?id=3063

24. ***June 25, SC Magazine*** – (International) **Study: 61 percent of critical infrastructure execs confident systems could detect attack in less than a day.** Tripwire released survey results from 400 executives in the energy, oil, gas, and utility industries in its “Critical Infrastructure Study” revealing that executives had high levels of confidence regarding their organizations’ ability to quickly detect cyber-attacks on their systems, while noting that attacks could seriously damage their infrastructure, among other findings.
Source: <http://www.scmagazine.com/critical-infrastructure-execs-recognize-companies-are-targets-believe-their-systems-can-quickly-detect-attacks/article/422676/>

25. ***June 25, V3.co.uk*** – (International) **Android malware dominates mobile threat landscape.** Pulse secure released findings from its Mobile Threat Report revealing that 97 percent of mobile malware is targeted at Android devices, and that in 2014 almost 1 million individual malicious apps were released. The report also highlighted the dangers in jailbroken and non-jailbroken iOS devices, among other findings.
Source: <http://www.v3.co.uk/v3-uk/news/2414871/android-malware-dominates-mobile-threat-landscape>

26. ***June 24, SC Magazine*** – (International) **Cyber-crime economy triggers rise in malicious macros.** Proofpoint released The Cybercrime Economics of Malicious Macros report, revealing that malicious macro campaigns have grown in size, frequency, sophistication, and effectiveness while increasingly relying on inexpensive vectors and techniques to exploit the human factor, among other findings.
Source: <http://www.scmagazineuk.com/cyber-crime-economy-triggers-rise-in-malicious-macros/article/422479/>

27. ***June 24, SC Magazine*** – (International) **MacKeeper flaw enables attacker to run code with admin rights.** Security researchers discovered a serious vulnerability in ZeoBit’s MacKeeper utility program in which an attacker could use a phishing email

containing a malicious link that prompts a user for a password, effectively executing the malware with administrator rights. ZeoBit reportedly acknowledged and patched the vulnerability.

Source: <http://www.scmagazineuk.com/mackeeper-flaw-enables-attacker-to-run-code-with-admin-rights/article/422516/>

28. *June 24, SC Magazine* – (International) **COA Network breached, all customer data treated as potentially compromised.** New Jersey-based COA Network Inc., reported that it had detected a pattern of irregular activity in its systems June 5, and is considering all customer contact and payment information as possibly having been compromised. The company took actions to increase security and protect customer information, and has notified all customers.
Source: <http://www.scmagazine.com/coa-network-breached-all-customer-data-treated-as-potentially-compromised/article/422637/>
29. *June 24, Softpedia* – (International) **ESET patches scan engine against remote root exploit.** ESET pushed an update for its scan engine addressing a vulnerability in antivirus products' code emulator component in which an attacker used a remote root exploit to take complete control of a system. NOD32 Antivirus, Microsoft Windows, Apple OS X, Linux, and numerous other consumer and business antivirus solutions, utilize the product.
Source: <http://news.softpedia.com/news/eset-products-vulnerable-to-remote-root-exploit-485191.shtml>
30. *June 24, Help Net Security* – (International) **Deadly Windows, Reader font bugs can lead to full system compromise.** A security engineer with Google Project Zero shared the discovery of 15 flaws in font engines used by Microsoft Windows, Adobe Reader, and other popular software that could allow an attacker to compromise systems in a variety of ways including creating an exploit chain leading to a full-system compromise. All of the reported vulnerabilities have been patched in recent updates.
Source: <http://www.net-security.org/secworld.php?id=18549>
31. *June 24, Securityweek* – (International) **Visibility challenges industrial control system security: survey.** Findings from a SANS Institute survey of over 314 respondents across several industries that interact with industrial control systems (ICS) revealed the perceived threats posed by internal and external attackers and the challenges of ICS protection. Challenges cited include poor optimization of ICS protection for information technology (IT) environments, the difficulty in detecting threats that spread without affecting operations, and the integration of IT into previously isolated ICS platforms, among other findings.
Source: <http://www.securityweek.com/visibility-challenges-industrial-control-system-security-survey>

For another story, see item [15](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

32. ***June 24, WPVI 6 Philadelphia*** – (Pennsylvania) **Verizon wireless service restored in Pennsylvania, New Jersey and Delaware.** Severe storms June 23 across Pennsylvania, New Jersey, and Delaware caused a 9-hour cellular phone service outage for Verizon Wireless customers, which included calls from cell phones to 9-1-1 voice services. Services have since been fully restored.
Source: <http://6abc.com/weather/verizon-wireless-service-restored-in-pa-nj-del/802810/>

For additional stories, see items, [24](#), [25](#), [28](#) and [31](#)

[\[Return to top\]](#)

Commercial Facilities Sector

33. ***June 25, KTVI 2 St. Louis*** – (Missouri) **Fire sweeps through Brentwood apartment complex.** The Brentwood Forest Condos in Brentwood, Missouri evacuated all 8 apartment units June 25 after a fire started on a second-story deck. No injuries were reported and the cause of the fire is under investigation.
Source: <http://fox2now.com/2015/06/25/fire-sweeps-through-brentwood-apartment-complex/>

34. ***June 24, WHNT 19 Huntsville*** – (Alabama) **86 sick in potential outbreak at 2 Montgomery day care centers.** The Alabama Department of Public Health announced June 24 that an investigation is ongoing to determine the cause of a widespread illness after 86 children fell ill while attending 2 different day care centers in Montgomery County. Parents are advised to avoid the day care centers until the investigation is complete.
Source: <http://whnt.com/2015/06/24/86-hospitalized-in-potential-outbreak-in-2-montgomery-day-care-centers/>

35. ***June 24, Lansing State Journal*** – (Michigan) **70 homes, many businesses damaged in tornado.** Ionia County, Michigan declared a state of emergency after a June 22 tornado heavily damaged 70 homes, more than 12 businesses, and at least 4 churches. Clean-up crews were deployed and repairs to the city are ongoing.
Source: <http://www.lansingstatejournal.com/story/news/local/2015/06/23/update-homes-many-businesses-damaged-portland-tornado/29163575/>

36. ***June 24, Bloomsburg Press Enterprise*** – (California) **Lake fire: 33-square-mile blaze expected to burn into July.** A June 24 lake fire prompted the evacuation of about 360 youth and staff at Camp Oakes as well as 2 mountain communities, after a wind shift caused the fire to change directions towards Onyx Peak, California. No injuries were reported.

Source: <http://www.pe.com/articles/fire-771332-lake-spread.html>

37. ***June 24, KOIN 6 Portland*** – (Oregon) **25 tenants displaced in Salem apartment fire.**

A 3-alarm fire at a Salem, Oregon apartment complex displaced approximately 25 residents after the fire destroyed 8 apartment units June 24. Fire crews contained the incident and no injuries were reported.

Source: <http://koin.com/2015/06/24/25-residents-displaced-in-salem-apartment-fire/>

38. ***June 24, Time Warner Cable News*** – (New York) **Bomb threat forces evacuation of multiple downtown Syracuse buildings.** The Onondaga County Civic Center in Syracuse, New York was evacuated and closed for more than 3 hours June 24 after 2 phone-in bomb threats prompted officers and canine crews to inspect the building. No threats were found.

Source: <http://www.twcnews.com/nys/central-ny/news/2015/06/24/onondaga-county-bomb-threat.html>

[\[Return to top\]](#)

Dams Sector

Nothing to report

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.